Internationalization and ICT Law

Koops, E.J.; Prins, J.E.J.

Published in:
Computer Law and Security Review

Publication date:
2000

PUBLIC ICT POLICY

INTERNATIONALIZATION AND ICT LAW: THE POSITION OF THE UK, GERMANY, FRANCE AND THE UNITED STATES[1]

Bert-Jaap Koops and Corien Prins[2]

The information society is essentially an international society. This challenges the law, which is still to a large extent nationally-based. The prime question that thus arises is: how can and should governments regulate information and communications technologies (ICT) and the Internet, given the fundamental influence of internationalization? The Center for Law, Public Administration and Informatization of Tilburg University (The Netherlands) researched the points of view on this of the governments of France, Germany, the United Kingdom, and the United States, focusing on a number of general themes and specific issues in private and criminal law. The research was commissioned by the Dutch Ministry of Justice to support their memorandum *Internationalization and the law in the information society*, presented to the Dutch Parliament in May 2000. The research took place from January through April 2000 by analysing the states' major ICT policy papers and laws and by an international workshop held in Amsterdam. The outcome suggests that, if ICT law wants to grow up, governments should structurally incorporate the perspective of internationalization and jurisdiction in all policy-making in the area of ICT law.[3]
This article discusses the key issues that were addressed in the above-mentioned research and presents the main conclusions that were drawn.

INTRODUCTION: TOPICS AND RELEVANT DOCUMENTS

Given the fact that numerous issues could be researched when it comes to the question how to regulate ICT in light of the fundamental influence of internationalization, the research was focused on a particular number of general themes and specific issues in both private and criminal law. As regards the general themes, the study covers the issues of self-regulation, the adage "what holds offline should also hold online" and enforcement. In addition four specific subjects were covered, all of which are on the agenda today: judicial cooperation in criminal matters, the requirement of double criminality for context-dependent offences, civil liability of ISPs and finally, the question which law applies to online agreements. All issues were researched in light of the positions of the governments of France, Germany, the United Kingdom, and the United States.

Since the mid-nineties, numerous policy documents have been published in the above countries. To give the reader a hand in finding these documents, we mention at this point the key documents:

Germany

As regards Germany the following documents are relevant:

- Bundesministerium für Wirtschaft, Info 2000: Deutschland's Weg in die Informationsgesellschaft, February 1996, WWW < http://www.bmwi-info2000de/ archive/berichte/info2000/index.html>
- Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie, Multimedia möglich machen. Deutschlands Weg in die Wissensgesellschaft, february 1999, WWW <http://www.iid.de/mmm_ bmbf/mm_ p4.htm>.
- Bundesministerium für Wirtschaft und Technologie, Evaluierungsbericht des IuKDG, 16 June 1999, WWW <http://www.iid.de/iukdg/pm160699.html>.
- Innovation und Arbeitsplätze in der Informationsgesellschaft des 21. Jahrhunderts – Aktionsprogramm der Bundesregierung, 1999, <http://www.iid.de/aktionen/aktionsprogramm/deckblatt.html>.
- Schlußbericht der Enquete-Kommission Zukunft der Medien in Wirtschaft und Gesellschaft – Deutschlands Weg in die Informationsgesellschaft zum Thema Deutschlands Weg in die Informationsgesellschaft, 22 June 1998, Druksache 13/11004.

ISSN 0267 3649/00/$20.00

The United Kingdom

The position of the UK is reflected among others in the following documents:

- John Battle, *HMG Strategy For the Internet*, 18 March 1998, WWW <http://www.dti.gov.uk/Minspeech/btlspch3.htm>.
- Tony Blair, *Our Information Age, The Government's Vision*, May1998, WWW <http://www.number-10.gov.uk/textsite/info/releases/publications/infoagefeat.html>.
- Cabinet Office, *E-commerce@its.best.uk*, September 1999, WWW <http://www.cabinet-office.gov.uk/innovation/1999/ecommerce/index.htm>.
- House of Lords, *Information Society: Agenda for Action in the UK*, 23 July 1996, WWW <http://www.parliament.the-stationery-office.co.uk/pa/ld199596/ldselect/inforsoc/inforsoc.htm>.
- House of Commons, *Tenth Report of the Select Committee on Trade and Industry*, August 1999, WWW <http://www.parliament.the-stationery-office.co.uk/pa/cm199899/cmselect/cmtrdind/648/64802.htm>.
- *The Government's policy for the information age*, WWW http://www.isi.gov.uk/isi/infosoc/govpolicy.htm
- Judicial Cooperation Unit, *Seeking Assistance in Criminal Matters from the United Kingdom. Guidelines for judicial and prosecuting authorities (Second Edition)*, October 1999, WWW <http://www.homeoffice. gov.uk/oicd/jcu/guidelns.htm>.

France

As regards the position of France we mention the following documents:

- Comité Interministériel pour la Société de l'Information, Mise en oeuvre du Programme d'action gouvernemental pour la société de l'information – Etat d'avancement après un an (janvier 1998 – janvier 1999), 19 January 1999, WWW <http://www.internet.gouv.fr/francais/textesref/cisi190199/sommaire.htm>.
- Conseil d'Etat , Internet et les résaux numériques, 2 July 1998, WWW <http://www.internet.gouv.fr/francais/textesref/rapce98/synthese.htm>.
- Prime Minister, 'Preparing France's Entry into the Information Society', 25 August 1997, WWW <http:// www.premier-ministre.gouv.fr/GB/INFO/HOURT.HTM>.
- Le Premier Ministre, Société de l'information: discours du Premier ministre à l'Université d'été de la communication, Hourtin, 26 August1999, WWW <http://www.internet.gouv.fr/francais/textesref/pagsi2/discourspm.htm>.
- Le Premier Ministre, Allocution du Premier ministere lors de la réception concluant la conférence mondiale des régulateurs sur l'internet, Paris, 1 December 1999, WWW <http://www.premier-ministre.gouv.fr/PM/D011299.htm>.
- Ministère de l'Économie, des Finances en de l'Industrie, Francis Lorentz, Commerce électronique. Une nouvelle donne pour les consommateurs, les entreprises, les citoyens et les pouvoirs publics, 7 January 1998, WWW <http://www.finances.gouv.fr/lorentz/rapports/index-d.htm>.
- Ministère de l'Économie, des Finances en de l'Industrie, Francis Lorentz, Rapport sur le commerce électronique – Addendum, 15 March 1998, WWW <http://www. finances.gouv.fr/lorentz/rapports/forum.htm>.
- Ministère de l'Économie, des Finances en de l'Industrie, Francis Lorentz, La nouvelle donne du commerce électronique. Réalisations 1998 et perspectives. Synthèse, February 1999, WWW <http://www.finances.gouv.fr/ lorentz/travaux/synth_generale.html>.
- Comité Interministériel pour la Société de l'Information, Programme d'action gouvernemental. Préparer l'entrée de la France dans la société de l'information, 16 January 1998, WWW <http://www.internet.gouv.fr/francais/textesref/pagsi.htm>.
- Dominique Strauss Kahn et al., Une société de l'information pour tous. Document d'orientation, November 1999, WWW <http://www.internet.gouv.fr/ francais/ index.html> (Engels: Policy Paper On The Adaptation Of The Legal Framework To The Information Society, WWW <http://www.finances.gouv.fr/ societe_information/anglais/sommaire_ang.htm>).

The United States

The position of the United States can be found among others in the following documents:

- William J. Clinton, *Presidential Directive*, 1 July 1997, WWW <http://www.whitehouse.gov/WH/New/Commerce/directive.html>.
- Department of Commerce, *Privacy and Selfregulation in the Information Age*, June 1997, WWW <http://www.ntia.doc.gov/reports/privacy/privacy_ report.htm>.
- Department of Commerce, *The Emerging Digital Economy*, April 1998, WWW <http://www.ecommerce. gov/emerging. htm>.
- *Justice Department comments to the FTC on Consumer Protection in the Global Marketplace*, 29 March1999, WWW <http://www.usdoj.gov/criminal/cybercrime/ftcconsu.htm>.
- Federal Communications Commission, *Digital Tornado: The Internet and Telecommunications Policy*, March 1997, WWW <http://www.fcc.gov/Bureaus/OPP/working_papers/oppwp29.pdf>.
- President's Working Group on Unlawful Conduct on the Internet, *The Electronic Frontier: the Challenge of Unlawful Conduct Involving the Use of the Internet* , March 2000, WWW <http://www.usdoj.gov/criminal/ cybercrime/unlawful.htm>.
- William J. Clinton & Albert Gore, Jr., *A Framework for Global Electronic Commerce*, 1 July 1997, WWW <http://www.whitehouse.gov/WH/New/Commerce>.
- The White House, *Memorandum for Heads of Executive Departments and Agencies*, 1 May1998, WWW <http://www.npr.gov/library/direct/memos/disputre.html>.
- The White House, *Memorandum for the Heads of Executive Departments and Agencies. Facilitating the Growth of Electronic Commerce*, 29 November 1999, WWW <http://www.whitehouse.gov>.
- The White House, *National Plan for Information Systems Protection*, 7 January 2000, verkrijgbaar via WWW <http://www.epic.org/security/infowar/ resources.html>.

GENERAL THEMES

Unlike the Dutch government, which published an overall analysis of ICT law in 1998 (*Legislation for the electronic highways*),[4] few comprehensive legal policy documents avail in the countries researched; only France has taken a similar effort with its *Policy Paper On The Adaptation Of The Legal Framework To The Information Society* of October 1999,[5] which is to lead to a draft law in 2000. Nevertheless, the general treatment of ICT law in view of internationalization in France, Germany, the UK, and the US is roughly the same. This holds, for instance, for the first general theme researched, the principle that "what holds offline, should also hold online". This is the basic starting point of Dutch policy. It is also explicitly mentioned in the policy of the UK,[6] whereas it can be derived implicitly from the policy documents and laws of France and Germany. However, the study indicated that in recent times, the adage has been put under pressure, because legislative initiatives on several specific issues show that it is not always followed. Increasingly, certain interests — such as consumer protection, legal certainty, stimulating electronic commerce — call for specific rules for the online world that differ from those in the offline world. This tendency is also mirrored at the international level, e.g., in the European Union.

It is true that the adage "what holds offline, should also hold online" was a useful concept in the 'early days' of ICT law (in the mid 1990s), when it had to be made clear that the Internet was not a legal vacuum. Now, however, it appears rather a romantic, outdated concept. The complexity of the matter proves that the problems in the online world differ from those in the offline world. Therefore, it is unwise to take as a starting point the concrete rules of the offline world when thinking about regulating the online world. Rather, the *levels of protection* (and thus not the rules as such) should be the same in both worlds (as US policy documents mention). Governments should pay more attention to the interests and goals underlying the rules of the offline and online worlds. The question is *why* we have certain rules in the offline world, and *why* such rules should be maintained online. Rather than rely on transposing traditional rules or principles, governments had better forget the adage and be simply creative in finding solutions to the specific problems of the online world. One must also bear in mind the possibility that the adage "what holds offline, should also hold online" may be turned into its reverse: "what holds online, should also hold offline". Thus, the legislature must view the relationship between offline rules and online rules as an interactive one.

The second general theme of the research is self-regulation. The Dutch government has appeared a fervent adherent of self-regulation mechanisms in solving legal uncertainty about the consequences of cross-border electronic communications. In choosing self-regulation, the government hopes to create sufficient flexibility in a time of technological and societal turbulence. Also, self-regulation is, in principle, not bound by borders. Nevertheless, government regulation is still the starting point if fundamental values of the rule of law are at stake — the Dutch government here refers to the classic fundamental civil rights, to preventing and investigating breaches of the rule of law and of state security, as well as to consumer protection, privacy, and the issue of applicable law.

The research shows that self-regulation is likewise a central theme in the various policy documents of the countries as well as of international organizations. Also, more or less the same issues are mentioned when it comes to a preference for government intervention (in particular, fundamental rights and values, consumer protection, law and order, state security).

Despite the broad support for self-regulation, the study shows that there is a remarkable tendency in all countries. Whereas the governments used to take the point of view that government intervention was, in principle, undesirable and that the market should lead, there is increasing awareness that governments cannot restrict themselves to solely stimulate; shaping E-commerce policy and Internet policy is a task for government and market together. 'Co-regulation' is a term that appears prominently in many recent policy documents. In France, the government has established a special organ for co-regulation ('organisme de corégulation'), chaired by Parliamentary representative Christian Paul.[7] Even in the US, the general opinion seems to lean towards the view that the government should play a more guiding role than it used to do in shaping the policy. One must bear in mind, however, that the term 'co-regulation' is not interpreted the same way in the various countries. The interpretation depends to a large extent on legislative and cultural traditions. When governments talk about co-regulation, they are therefore prone to talk about different things.

In thinking about the necessity of government intervention, it may be useful to distinguish between regulation that aims at answering practical questions ("Can I use a digital signature to make a transaction?") and regulation that aims at influencing behaviour ("Don't use encryption that hampers law enforcement!"). The first kind of regulation is generally called for and welcomed by the market, whereas the second kind is generally not favoured.

When deciding both what rules should apply in the online world and what level of regulation can best shape these rules, the enforcement of the resulting regulation is of crucial importance. Especially in an international context, enforcement of regulation is a problematic issue. This, then, is a third general theme that pervades ICT law.

In the policy documents, the question of how to safeguard enforcement is less prominent than the first two general themes. Although governments have put considerable thought to the necessity and options of ensuring enforcement of ICT law in the international context, so far, they have not put forward ideas about an integral approach to enforcement. They simply look for the best approach in each given case, which is in line with the Dutch pragmatic approach in this matter. It is also remarkable that there are few concrete ideas about how to address at an international level those issues generally considered to be potentially difficult to enforce in an international context, such as tax law, privacy, and cryptography.

In those areas where the interests to be protected are broadly shared internationally, there will be the best likelihood of an international approach. It is wise to start with small domains on which there is more agreement, e.g., in combating child pornography, for which an international network of hotlines is already at work.[8] Constructions of national contact points are the most promising in the short term to address enforcement internationally. In private-law matters, one can think of an international network of ombudspersons or the Chambers of Commerce to play a central part in international online alternative dispute resolution. In criminal law, for the time being, states concentrate

on an international network of national contact points available 24 hours a day and seven days a week to directly deal with and coordinate requests for mutual criminal assistance. This network can give an impetus to further-reaching forms of cross-border cooperation.

SPECIFIC ISSUES

Besides these general themes, we researched as mentioned above, four specific issues, two in criminal law and two in private law.

The first issue in criminal law is **double criminality**, which is usually required for mutual assistance in criminal matters. In the memorandum *Legislation for the electronic highways*, the Dutch government suggested that this requirement could perhaps be dropped under certain conditions in cases where a state requests another state to provide information in order to be able to follow a digital trace.

There is no indication that other countries think about abandoning the requirement of double criminality. It is true that within the Council of Europe, it is discussed, but overall their draft *Convention on Cyber-Crime* (usually referred to as *Crime in Cyberspace*)[9] does not initiate discarding double criminality. Although the text seems to suggest that the requirement must not or need not be absolute, there is no consensus on this among the participating states. Moreover, the abandonment of double criminality as discussed is restricted to *preserving* data in another country; it does not stretch to *providing* those data, and so, the requirement will at all counts continue effectively to exist.

Likewise, the discussion at the international workshop did not support relinquishing the requirement of double criminality. The foreign experts appeared surprised rather than stimulated to think about the idea. Double criminality seemed to them to be so fundamental, that there is or should be in fact no possibility to undermine it in any way.

Given the fact that abandoning double criminality in any way is not favoured internationally, and because of the fact that in most cases it is hardly realistic to harmonize material criminal laws, the international fight against ICT crime will have to resort to cooperation between enforcement authorities.

The Dutch government's view on this second issue, cooperation between enforcement authorities, is that there must be rules that ensure effective cooperation, especially to regulate investigation powers aimed at foreign Internet providers and to ensure the cooperation of other states to facilitate investigation. In particular, the government stated in its 1998 memorandum that the draft treaty *Crime in Cyberspace* should enable judicial authorities to directly address foreign network providers, without prior mediation of investigation authorities in the country of the network provider. Court supervision could take place afterwards.

The necessity of closer cooperation between enforcement authorities is recognized in the other countries. Governments acknowledge that to achieve this, traditional mutual assistance will have to be adapted drastically. They see this primarily as a problem for which solutions have to be found at an international level. Therefore, this issue is discussed mainly in international platforms; on the national level, no conclusive steps are taken before the results of the international discussions become clear.

At a national level, states restrict themselves to short-term measures, like establishing continuously accessible contact points, and to other means available within the present legal framework. The Dutch desire to make it easier to gain access to foreign data seems to be in line with the thinking in other countries, but foreign governments have not yet published positions about the specific desire to get data directly from foreign Internet providers.

Moreover, the draft convention *Crime in Cyberspace* of the Council of Europe does not contain a proposal to this effect. It does propose a new investigation power: a preservation order to telecoms or Internet providers that can be easily given and that safeguards the availability of the data pending the exercise of other investigative powers, such as a 'search and seizure' of data. However, for preserving data stored in another state, authorities will still have to make a traditional request for criminal assistance — a request addressed to foreign providers directly was turned down in the draft convention.

The first specific issue in private law we researched is the topic of applicable law in international online contracts. The Dutch government attaches great value to clarifying the rules of private international law on which law applies. The Dutch government favours establishing a broadly formulated framework of private international law rules that apply to online contracts within the framework of the Hague Conference on private international law.

For the time being, this view does not seem to be shared in the countries we researched. In the US, the issue does not seem to play a part in policy-making at the federal level (bearing in mind that in the US, the issue of applicable law to online contracts can be addressed at the state level, which at present already raises enough problems). For Germany and the UK, we did not find government positions on this, whereas France has formulated a different position. The European countries seem to want to tie in with the rules of the (European) Rome Convention. The Netherlands, then, is leaning more towards a global solution than the other countries. One should note, however, that this approach does not seem to work out particularly smoothly. At a meeting in Ottawa in February 2000, it appeared scarcely realistic to agree upon the draft for adapting the Hague Conference.

The second issue in private law is **civil liability of Internet providers**. In Dutch law, tort is sufficiently technology-independent for the government to be able to leave it to the courts to develop this issue. Still, the government supports the European Commission in trying to establish common principles at an international level in order to create a level playing field. However, the Dutch government does not agree with all proposals on provider liability in the E-commerce Directive. In particular, the Minister of Justice questions the clarity of the distinction between the various categories of service providers (access, caching, and hosting providers). Moreover, he doubts the prudence of excluding beforehand access providers from liability regardless of whether they had knowledge of illegal content.

An analysis of the civil-liability position of Internet providers in the other countries shows that the material criteria used are similar, for instance, involvement with the content, knowledge, and due care. Providers that are involved with the content are fully liable, while those that are not are only liable if they do not conform with duties of care. In some countries, the latter

category further distinguishes between access providers and hosting providers. Generally, (non-content) providers are only liable for illegal content of which they have knowledge, with two exceptions. In Sweden, providers have a proactive duty to check material; since they can comply with this requirement by establishing a hotline, there is no obligation of result but only one of effort.[10] A second exception is the categorical exclusion, regardless of knowledge, of access providers in the German and EU regulations. Finally, a duty of care for service providers encountered everywhere is to remove or block access to illegal content as soon as the provider gains knowledge of it, at least as far as he is reasonably able to.

It is generally recognized that Internet service providers have a special role and responsibility to identify content providers. This may also stretch to preparatory measures like preserving data and verifying the identity of new subscribers. However, most governments are still struggling to find a balance between this requirement and the resulting infringement of privacy regulations.

There is sufficient space for regulating provider liability within each national state. However, to prevent major differences between the national regulations (which could impede international E-commerce), international harmonization is called for, hence the regulation in the European E-commerce Directive.

As to the international problems of illegal content — addressing content that is illegal in a country but that is hosted abroad — the general position of governments is one of reserve. States do not view provider liability a good way to address this (it is interesting to note that Australia and Singapore are exceptions to this, with regulations that put obligations on national providers with respect to content hosted abroad)[11]. For the time being, states take recourse to stimulating international cooperation between private-sector hotlines.

DISTINCTIONS AND TRADE-OFFS

Aside from the various insights in the dimensions of internationalization in national policy-making, the findings of the research suggest that several distinctions and trade-offs are relevant to creating ICT-law policies.

Offline – online

The adage "what holds offline, should also hold online", a useful concept in the early days of ICT law, appears not to be generally applicable anymore. It is still relevant in relation to the interests and the level of protection that underlie the rule systems of the offline and online worlds, but rather than focusing on transposing the offline rule system to the online world, governments should focus on the specificity of the problems in the online world.

Government regulation – Self-regulation

The general preference for self-regulation that until recently pervaded thinking about ICT law is generally giving way to a preference for co-regulation, since governments have come to the conclusion that safeguarding crucial interests and legal certainty calls for a more prominent role of governments. This new balance between government and market regulation is termed co-regulation everywhere, but the specific interpretation of this term varies per country. Some countries put more stress on the government side, and others on the market side, largely because of their cultural and legislative traditions. This influences, among others, the choice of a voluntary or an obligatory enforcement mechanism. From an international perspective, it is important to be aware of the variation in the views on co-regulation and in the underlying national values.

Overall principles – Specific solutions

Governments had better concentrate on finding a tailor-made solution to each specific issue requiring regulation rather than try to define general guidelines and principles for the broad field of ICT law. General principles (such as an overall preference for self-regulation and 'offline = online') do injustice to the specific problems of all the various issues. In order to make clear the government position in international platforms, it may be useful to define certain general positions that mirror national interests and traditions, but this holds the risk that national governments sticking to their general position as outlined hamper the search for a creative solution. It is more important in international platforms for governments to have an open attitude that takes into account other valid approaches and principles.

Answering – Steering

Conceptually, one can distinguish between regulations that primarily try to answer practical questions in order to create legal certainty (e.g., "can I use a digital signature to sign a contract?") and regulations that aim at influencing behaviour (e.g., "do not use encryption that hampers investigation"). With 'answering issues', the addressees, in principle, care less about the particular outcome as long as a choice is made by the government, whereas with 'steering issues', addressees have a clear preference for a particular outcome. It is true that regulation is never completely answering or completely steering, but in most cases, there is an emphasis on one side or the other. This affects the likelihood of compliance, the enforcement options, and therefore the effectiveness of the regulation. In the short term, primarily answering regulations are called for in order to establish legal certainty, whereas more steering regulations should only be undertaken once it has become sufficiently clear what 'steering goals' are envisioned and what are the best means to achieve those goals.

Top-down – Bottom-up

Certain topics, such as Internet-provider liability and electronic signatures, are essentially national issues that can be addressed at a national level. Given internationalization, however, these national regulations must be tuned to one another, which is done at an international level. The resulting interaction between national and international actions is not always optimal, because states sometimes at an early stage create national legislation that significantly diverges from solutions proposed internationally. Other topics call for an international approach by definition, such as applicable law in online contracts and cross-border satellite eavesdropping. In these areas, policies are nearly always made at the international level, which carries a risk that national governments will not publish their opinions and that no national

debate will take place on these topics. This can also hamper the interaction between national and international policy-making. Both the primarily bottom-up issues and the primarily top-down issues, then, require governments to be more aware of the international dimension of the policies under discussion, and to optimize the interaction between national and international policy-making.

CONCLUSIONS

What conclusions can be drawn from the analysis in the study? We discern a desire for a uniform approach of the various problems, but at the same time a need to be aware of the specific dynamics of each issue, the range of interests involved, and the variety of cultural and legislative national traditions. In short, there must be variety in unity.

This means that in various areas, international agreement can be problematic. The creative approach that is needed implies in the first place a search for areas where the interests are mutual and where it is relatively easy to reach agreement. Once governments agree upon the major points in this area, topics could be addressed where the positions diverge more. The broad field of ICT law must thus be addressed slowly, step by step.

It is of primary importance that each issue is indeed addressed from an international perspective. Our research indicates that the thinking about ICT law is still taking place to a large extent from a national perspective. This is not surprising in the light of the 'growing-up' of ICT law, but it is undesirable to keep the international perspective out of sight any longer. Questions of internationalization and jurisdiction are so intrinsic to policy-making in the area of ICT law, that the national and international perspectives cannot do without each other.

We think the time has come to take the next step forward in regulating the electronic highway. Five years ago, policy concentrated on addressing national problems. Now that this approach is well on its way, it is time for the next step: including the international dimension of the problems. Although governments currently proclaim that international policy fine-tuning is needed, our analysis shows that in reality, few things come off the ground, and that it is often noted that problems should first take shape at a national level. There are many initiatives by international organizations, but these have yielded few concrete results so far. In short, both at the national and at the international level, there is little effective progress in policy-making from the perspective of internationalization and jurisdiction.

Therefore, the international community should structurally pay attention to the perspective of internationalization and jurisdiction in all the platforms that discuss ICT-law issues. Also, policy-making in all the various international institutions and platforms must be better tuned. In order to facilitate the international discussions in which it takes part, governments can formulate rules of thumb that support their positioning, but these can be no more than starting points for discussion. First and foremost, and even more so than with traditional law topics, the government should have a flexible and particularly open attitude that discerns and pays attention to all the nuances of the issue at stake and the variety of national positions that are intrinsic to the internationalization problems related to ICT law.

The final conclusion is that governments should incorporate the international dimension more emphatically in the national and international policy-making in the field of ICT law. ICT law has by now outgrown the infancy stage of general starting points and national interim solutions. A grown-up ICT law calls for structurally incorporating the perspective of internationalization and jurisdiction.

Dr. Bert-Jaap Koops and **Prof. dr. Corien Prins**
Center for Law, Public Administration and Informatisation
Tilburg University

FOOTNOTES

[1]This article is based on a report written for the Dutch government (see: footnote 2). In addition to the authors of this article, the following persons participated in the project: Maurice Schellekens, Serge Gijrath and Eric Schreuders.

[2]Dr. Bert-Jaap Koops is a senior researcher with the Center for Law, Public Administration and Informatisation at Tilburg University. Prof. dr. Corien Prins is a professor of law and informatization with the aforementioned Center.

[3]The report is available in Dutch at WWW <http://rechten.kub.nl/crbi/rapport.pdf>. An English version will be published, together with the Dutch government's memorandum on internationalization, with Kluwer Law International.

[4]Kamerstukken II, 1997-1998, 25 880, nrs. 1-2.

[5]Dominique Strauss Kahn et al., *Une société de l'information pour tous. Document d'orientation*, November 1999, WWW <http://www.internet.gouv.fr/francais/index.html> (English: *Policy Paper On The Adaptation Of The Legal Framework To The Information Society*, WWW <http://www.finances.gouv.fr/societe_information/anglais/sommaire_ang.htm>).

[6]John Battle, *HMG Strategy For the Internet*, 18 March 1998, WWW <http://www.dti.gov.uk/Minspeech/btlspch3.htm>.

[7]<http://www.internet.gouv.fr/francais/textesref/pagsi2/lsi/coregulation.htm>.

[8]<http://www.inhope.org>.

[9]Council of Europe, *Crime in Cyberspace. First Draft of International Convention Released for Public Discussion*, 27 April 2000, WWW <http://conventions.coe.int/ treaty/ en/projets/cybercrime.htm>.

[10]Lag (1998:112) om ansvar för elektroniska anslagstavlor. See: J. Palme, Swedish Law on Responsibilities for Internet Information Providers, 1998 <http://www.dsv.su.se/ ~jpalme/society/swedisch-bbs-act.html>

[11] In Australia the Broadcasting Services Amendment Bill 1999 contains the relevant rules (see on this Bill: B. Scott, 'An Essential Guide to Internet Censorship in Australia', *World Internet Law Report*, 1999/10, p. 16-21. In Singapore the rules are stipulated in art. 10 of the Electronic Transactions Act 1998 (see: S.B. Hogan, 'To Net or Not To Net: Singapore's Regulation of the Internet', *Federal Communications Law Journal*, 1999, p. 429-447; <http://www.law.indiana. edu/fclj/pubs/v51/no2/v51no2.html>.